REMARKS

The Office Action dated March 16, 2005 has been received and carefully noted. The following remarks are submitted as a full and complete response to the Office Action.

Applicant gratefully acknowledges the indication that claims 43-57 would be allowable if rewritten in independent form. It is respectfully submitted that these claims are allowable in their present form. Claims 33-68 are respectfully submitted for consideration.

Claims 33-42, and 58-68 have been rejected under 35 U.S.C. § 103(a) as being obvious over U. S. Patent No. 5,642,401 to Yahagi (Yahagi), in view of U.S. Patent No. 5,991,407 to Murto (Murto). The Office Action took the position that Yahagi discloses all of the features recited in the above-identified claims except the feature of a plurality of messages selected from a set of message types, and asserts that Murto discloses this feature. This rejection is respectfully traversed.

Claim 33, upon which claims 34-43, 49, 54-56 and 58-62 depend, recites a method of securing communication between a first party and a second party in a telecommunications network. The method includes the step of defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The method also

includes the steps of selecting one of the plurality of different security methods in accordance with defined criteria and performing the security method.

Claim 63 recites a telecommunications network element for securing communication between a first party and a second party. The network element includes means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each including a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The network element also includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria and means for insuring that the communication between the first and second parties is in accordance with the selected security method.

Claim 64 recites a terminal for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The terminal further includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and means for ensuring that the communication between the first and second party is in accordance with the selected security method.

Claim 65 recites a system for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of

different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The system further includes a selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and a means for ensuring that the communication between the first and second party is in accordance with the selected security method.

Claim 66 recites a computer program product comprising computer-readable code, the computer-readable code causes a computer to perform a procedure for securing communications between a first party and a second party including a means for defining a criteria for selecting one of a plurality of different security methods, the plurality of security methods each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common. The computer code further includes selection means for selecting one of the plurality of different security methods in accordance with the defined criteria, and a means for ensuring that the communication between said first and second party is in accordance with said selected security method.

Claim 67 recites a method of securing communication between a first party and a second party in a telecommunications network including the steps of defining a criteria for selecting one of a plurality of different security methods each having a different set of steps for performing the respective security methods, the plurality of security method each comprising a plurality of messages selected from a set of message types, at least two

different security methods having at least one message in common. The method further includes selecting one of the plurality of different security methods in accordance with the defined criteria, and performing the security method.

Claim 68 recites a method of securing communication between a first party and a second party in a telecommunications network including the steps of defining a criteria for selecting one of a plurality of different security methods each having a different set of steps for performing the respective security methods, the plurality of security method each comprising a plurality of messages selected from a set of message types, at least two different security methods having at least one message in common, selecting one of the plurality of different security methods in accordance with the defined criteria, and performing the security method.

According to embodiments of the present invention, the first party and second party may be a mobile station and a base station. The set of message types may include messages such as random number messages, hash function messages, signature function messages, parameters for use with function messages, security parameter messages, keys for function messages, encoded messages, messages to and/or from a third party and authentication response messages. These are all particular message types that may be used in authenticating a mobile station for use in a communication network. Thus, it is possible to select from a large number of different security methods. Applicant respectfully submits that the references cited in the Office Action fail to provide at least the above-discussed non-obvious advantages of the claimed invention.

It is respectfully submitted that the claimed invention advantageously allows a relatively large number of different security methods to be implemented using only a small number of different messages. As shown at least in Figures 3 – 9, the claimed invention comprises a plurality of different security methods. Accordingly, independent claims 33 and 63-68 recite the feature of selecting a security method from a plurality of security methods. It is respectfully submitted that the references cited in the Office Action, taken either individually or in combination, fail to disclose or suggest the elements of any of the presently pending claims.

Yahagi discloses an "authentication algorithm calculation means 6 [that] performs an authentication calculation by using an authentication random number sent from a base station 2 and the authentication key 5 as input parameters" (column 3, lines 63-67). In Figure 3 thereof, Yahagi further discloses steps of a single authentication method which merely selects a random number from a plurality of random numbers. The Office Action admits that Yahagi does not disclose the feature of a plurality of messages selected from a set of message types and alleges that Murto discloses this deficiency.

Murto discloses an authentication procedure in a GSM-based mobile communications system. The Office Action relies on Murto to disclose the feature of a plurality of messages selected from a set of message types. Murto, similar to Yahagi, discloses a GSM authentication method involving selecting a random number RAND from a plurality of random numbers RAND(1...n) and calculating a respective authentication result SRES. More specifically, Murto discloses selecting one of a

plurality of "triplets" each comprising a random number RAND, an authentication result SRES and a ciphering key K_c (see column 5 lines 35-45 of Murto). These triplets are derived using pairs of values IMSI and Ki, (alleged plurality of message types).

Yahagi (col. 2 lines 7-24) merely discloses a single security method, which is a function of a random number. Specifically, Yahagi discloses that a single variable RAND[j] changes and effects the authentication result SRES (i.e. SRES = f(RAND[j]). Hence, Yahagi discloses a pair of values which are sent (SRES[1...n], RAND[1...n]) i.e. a random value and the authenticated result based thereon. Specifically Yahagi at col. 3 lines 63-67 states: "The authentication algorithm calculation means 6 performs an authentication calculation by using an authentication random number sent from a base station 2 and the authentication key 5 as input parameters." (emphasis added). The selection of a random number from a plurality of random numbers is not analogous to the selection of a security method from a plurality of security methods, as recited in the current claims. It is further submitted that Murto fails to make up for these deficiencies.

It is respectfully submitted that, the cited combination of references fails to disclose or suggest at least the feature of "defining a criteria for selecting a one of a plurality of different security methods", as recited in claims 33 and 63-68 of the present application. As discussed above, since Yahagi fails to disclose or suggest a plurality of security methods, Yahagi inherently fails to disclose defining a criteria for the selection of a method from a plurality of methods as recited in claims 33 and 63-68.

In addition, the Office Action alleges that Yahagi at column 3 lines 1-27 discloses the step of selecting one of the said plurality of different security methods in accordance with said defined criteria and performing said security method. It is respectfully submitted that Yahagi merely discloses that the security method is based on a random number and on an authentication key variable. However, Yahagi fails to even mention selecting between this security method and any other security method, much less defining a criteria for selecting between the different security methods, as recited in clams 33 and 63.

Applicant respectfully submits that Figures 3-9 of the present application illustrate various different examples of the "plurality of different security methods" recited in claims 33 and 63-68 of the present application. Applicant also respectfully submits that, as disclosed in the specification of the present application, the "criteria for selecting one of a plurality of different security methods" recited in claims 33 and 63-68 may include, for example, the processing capability of each of the two parties, or the time since the last security method was performed, as well as a random selection.

As discussed above, Yahagi discloses only the single security method illustrated in Figure 3. Applicant also points out that column 2 lines 7-24 and column 3 lines 1-17 of Yahagi, at best, merely disclose a single security method that utilizes a plurality of authentication random numbers and corresponding authentication calculation results. However, Applicant respectfully submits that these random numbers and calculation results are no more than messages in the authentication method illustrated in Figure 3 of

Yahagi. Hence, at least in view of the above, Applicant again points out that Yahagi fails to disclose or suggest at least the "defining" and "selecting" steps recited in the pending claim 33 and similarly recited in claims 63-68.

It is respectfully submitted that Murto fails to make up for the above-stated deficiencies of Yahagi, including the features alleged in the Office Action. Murto does not disclose the feature of a plurality of methods, as recited in the pending claims. The only variant aspects of Murto is the use of triplets, i.e., in the values of RAND, SRES and K_c that are used in each case. In fact, the only difference is in the value of RAND, since both SRES and K_c are calculated as a function of RAND (see column 5 lines 24030 wherein Ki is a parameter of a given subscriber). As discussed above regarding Yahagi, the use of a different random number does not constitute a different authentication method. Murto merely describes a single authentication method and makes no distinction in this method based on the values of the triplets.

In addition, even for the sake of argument only, if the triplets 1...n correspond to a plurality of methods there is no suggestion that the values RAND, SRES, and K_c of each triplet are selected from a plurality of method types, as recited in the present claims. In fact, in direct contrast, the entire plurality of triplets 1...n is derived from a single pair of values IMSI and Ki. See column 5 lines 44-45 of Murto "The file 40 contains n triplets 1 ...n for each IMSI subscriber."). The IMSI and authentication key Ki are both fixed for a given subscriber (see column 5 lines 13-16). Thus, IMSI and Ki are not considered to be different methods, as similarly discussed above regarding RAND, SRES and K_c.

Thus, it is respectfully submitted that the cited combination of references taken either individually or in combination fails to disclose or suggest all of the features recited in claims 33 and 63-68. Further, since claims 34-42 and 58-62 depend from claim 33, these claims are allowable at least for the same reasons as claim 33.

Furthermore, it is respectfully submitted that one skilled in the art would not be motivated to combine Yahagi with Murto to disclose the features recited in the present invention.

In order to establish a prima facie case for obviousness, there must be some teaching or suggesting tocombine the references. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

As discussed above, Yahagi discloses eliminating multiple random numbers RAND(1...n) and authentication results SRES(1...n), whilst Murto on column 3 lines 7-10 states "[a] further object of the invention is to enable the use of a CAVE algorithm as the A3 algorithm in the GSM system or in a GSM-based mobile communications network without modifications in the GSM triplet data structure" (underline added). Thus, one skilled in the art would not be motivated to combine the teachings of Yahagi with Murto. Accordingly, the Office Action has not established a prima facie case to support an obviousness rejection of the present claims.

It is respectfully submitted that the cited references taken either individually or in combination fails to disclose or suggest all of the features of the present invention and that a prima facie case for obviousness has not been established. Accordingly,

withdrawal of the rejection of claims 33-42 and 58-68 under 35 U.S.C. §103(a) is respectfully requested.

Applicants gratefully acknowledge the indication that claims 43-57 would be allowable if rewritten in independent form. However, Applicants submit that these claims are allowable in their present form at least for the same reasons as claims 33 and 63. Accordingly, withdrawal of the objection to claims 43-57 is respectfully requested.

Applicant respectfully submits that all of the comments included in the Office Action have been addressed and that all of the objections and rejections included in the Office Action have been overcome. Hence, Applicant respectfully further submits that, at least in view of the above, claims 33-68 of the present application contain allowable subject matter. Therefore it is respectfully requested that all claims pending in the present application be allowed, and that this application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the Applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

David E. Brown
Registration No. 51,091

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

DEB:mm

Enclosures: Petition for Extension Time